DOD PRIVACY IMPACT ASSESSMENT (PIA)
Sexual Assault Data Management System (SADMS)
(Use N/A where appropriate)

1. **Department of Defense (DoD) Component.**

   U.S. Army

2. **Name of Information Technology (IT) System.**

   Sexual Assault Data Management System (SADMS)

3. **Budget System Identification Number (SNAP-IT Initiative Number).**

   N/A

4. **System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).**

   DA03380

5. **IT Investment (OMB Circular A-l 1) Unique Identifier (if applicable).**

   N/A

6. **Privacy Act System of Records Notice Identifier (if applicable).**

   A0600–20 DCS, G–1

7. **OMB Information Collection Requirement Number (if applicable) and Expiration Date.**

   N/A

8. **Type of authority to collect information (statutory or otherwise).**

   Pub L 108-375, Section 577; 10 U.S.C. 3013, Secretary of the Army; DoD Directive 1030.1, Victim and Witness Assistance; AR 27-10 Military Justice; AR 40-66 Medical Record Administration and Health Care Documentation; AR 195-2 Criminal Investigation Activities; AR 608-18, Family Advocacy Program; AR 600-20, Army Command Policy; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; AR 600-20 (Chap 8), Sexual Assault Prevention and Response (SAPR) Program

9. **Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).**

   SADMS aggregates sexual assault-related data (to include personal identifying information (PII)) already captured in other Army systems; specifically the Army Criminal Investigation and Intelligence System (ACI2), Sexual Assault Response Program Tracking Application (SARPTA), Defense Case Record Management System (DCRMS) and Army Court Martial Information System (ACMIS). The data from these systems is provided to SADMS using several secure file transfer methods (e.g., Web Services; XML document up/download on secure site). Since sexual assault incidents involving uniformed service personnel may also involve non-DoD personnel as well, there is a distinct possibility that SADMS may also contain data in identifiable form on non-DoD personnel. It is clearly believed this will be the exception vice the rule though.

SADMS is a centralized repository of relevant data regarding the entire lifecycle of sexual assault cases, involving victims and/or alleged offenders who are members of the Armed Forces and to provide compilation of statistical data and management reports to enable Army SAPR Program leaders to assess the effectiveness of both response and prevention and make fact-based changes to policy and procedure on the strength of this analysis. SADMS "data collection" procedures and use authorizations from designated feeder systems are governed by data agreements between the Army G-1 and the functional organizations owning these systems. Final disposition instructions controlling how long this data can be held and when it must be destroyed are currently in the coordination process with the National Automated Records Archive (NARA). the Army intends to treat SADMS data as permanent records until NARA directs final disposition instructions.

The SADMS web application and data tables are all hosted on accredited US Army Information Technology Agency (USAITA) servers physically located in the basement of the Pentagon. Access to records in the SADMS is protected through assignment of user identification and passwords, which are required to be changed at random times, to protect the system from unauthorized access. The system employs a DoD Secure Socket Layer (SSL) certificate and encryption process to provide further protection from unauthorized access. All records are maintained in areas accessible only to authorized personnel who have an official need for access in order to perform their assigned responsibilities and duties. System-wide, SADMS employs separate database/web servers with restricted direct access to databases. Within the database server itself, databases are compartmented to specific logins. All traffic goes through a content filtering Raptor firewall and all Internet traffic also goes through the Pentagon's firewall.

10. **Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.).**

Name, Social Security Number (SSN), date of birth, demographic information, and Service data; investigation related information which may include summary of the assault, data from police reports, DNA processing dates; documents created as a result of the assistance provided; medical records data relating to initial and final treatment dates and aggregate count of intermediate medical treatment contacts with the victim; similar records/reports relating to victim support extended by installation and/or unit advocates; and reports of actions taken by commanders against offenders. This data is provided by the following systems - ACI2 (Army Criminal Investigation and Intelligence System), SARPTA (Sexual Assault Response Program Tracking Application), DCRMS (Defense Case Record Management System) and ACMIS (Army Court Martial Information System). As new IT systems are developed that may contain functional authoritative data deemed appropriate for integration into SADMS data records, Army G-1 will undertake appropriate coordination to develop data agreements with the appropriate agencies to further support data sharing with SADMS.

11. **Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).**

Records in this system are derived from data originally maintained in the following official Army systems: Army Criminal Investigation Intelligence System (ACI2); Sexual Assault Response Program Tracking Application (SARPTA); Defense Case Record Management System (DCRMS) (Army module); and Army Court Martial Information System (ACMIS). Selected data elements from each of these systems is provided via secure file transfer protocol (Secure FTP) or via Web Services transfer as designated within and

agreed to by the Army G-1 and the owning organizations in some combination of Memoranda of Agreement, Data Use Agreements and System Interface Agreements.

12. **Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.)**

On 6 Feb 04, the Acting Secretary of the Army (SecArmy) directed the establishment of an Army Task Force on Sexual Assault Policies to conduct a detailed review of the effectiveness of Army policies on reporting and addressing allegations of sexual assault and to review then-current processes to ensure a climate in which victims feel free to report allegations, and in which leaders understand their responsibilities to support victims and to investigate allegations. The task force report included a finding that the Army lacked an integrated approach for collecting, analyzing, and evaluating sexual assault cases. The report further noted that all available Army data on sexual assaults, victims, and alleged perpetrators reside in disparate systems across several Army organizations, and that this decentralization makes it difficult to follow victims, alleged perpetrators, and cases between Services, components, and organizations. To rectify this problem, the task force recommended the Army develop an integrated approach to case management and program assessment to facilitate data analysis and improvement of the recommended sexual assault prevention program. The Acting Secretary of the Army directed execution of an action plan to implementing the task force report recommendations on 19 Aug 04. On 28 Oct 04, the President signed Public Law 108-375, Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, Sec. 577, which mandated the development of a comprehensive DOD policy on the prevention and response to sexual assaults in the military, to include the uniform collection of data on the incidence of sexual assaults and on disciplinary actions taken in substantiated cases of sexual assault. Finally, DoD and Service SAPR policies as contained within DoDD 6495.01, Sexual Assault Prevention and Response (SAPR) Program and AR 600-20 (Chap 8), Sexual Assault Prevention and Response (SAPR) Program provide guidance supporting collection of sexual assault incident information that may include information in identifiable form.

13. **Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).**

Personally identifying information (PII) (e.g., Name, SSN, DOB) are the common data elements to each of the data systems identified in the Acting SecArmy TF Report on Sexual Assault Policies and is the basis upon which integration of these different data threads is executed. Using this PII most effectively ensures accurate correlation and maintenance of data integrity.

SADMS will primarily be used to provide a compilation of statistical data and management reports to enable Army SAPR Program leaders to assess the effectiveness of both response and prevention and make fact-based changes to policy and procedure on the strength of this analysis. Moreover, since SADMS is an integration of other system data, it affords HQDA level program managers to determine if all SAPR program component systems (i.e., law enforcement, medical, advocacy, chain of command, legal) are properly and/or effectively executing the program IAW existing policy guidelines.

14. **Describe whether the system derives or creates new data about individuals through aggregation.**

No personal information is derived or created as a result of this integration; the principle purpose of this data integration is to enable designated Army leaders to rapidly assess how well the Army SAPR Program is

meeting its mission of ensuring victims of sexual assault receive the services they need and desire and perpetrators of these offenses are held accountable for their actions.

SADMS is a consolidation of sexual assault incident and response data previously reported and captured in other Army information systems designed to provide Army SAPR program leaders a holistic view of these incidents, to measure the effectiveness of the Army's SAPR Program and to support the management of the program as recommended by the Acting Secretary of the Army's Task Force Report on Sexual Assault Policies published in May 2004.

15. **Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).**

The Army's intent is not to share information in identifiable form unless a requester's need to know is at least equal to, if not greater than, the potential impact of divulging the information, and that disclosure is otherwise consistent with law and regulation. No information in identifiable form contained within SADMS will be disclosed in response to internal Army requests for information unless specifically approved for release first by the functional system owner(s) of the data and then by either the Assistant Deputy Chief of Staff, G-1 or the Deputy Assistant Secretary of the Army for Human Resources, both members of the Senior Executive Service (SES).

SADMS information will not be used to inform or influence command or legal process decisions with respect to either victims or offenders. Unauthorized disclosure, unauthorized retention, or negligent handling of personal identifying information will not be tolerated and personnel responsible for this disclosure may be subject to criminal prosecution under federal law or the Uniform Code of Military Justice. Except as provided for in the Freedom of Information Act, PII within the system is not accessible by the general public. To the extent permissible under the law, information within the system will not be released to the public.

16. **Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.**

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to Deputy Chief of Staff, Army G-1, ATTN: FOIA/PA Officer , 300 Army Pentagon, Washington, DC 20310-0300

Individuals seeking access to information about themselves contained in this system should address written inquiries to the Deputy Chief of Staff, Army G-1, ATTN: FOIA/PA Officer , 300 Army Pentagon, Washington, DC 20310-0300.

The Army's rules for accessing records, and for contesting contents and appealing initial agency determinations are contained in Army Regulation 340-21; 32 CFR part 505; or may be obtained from the system manager.

Sexual assault victims can preserve and protect their own identity by electing to make their report of a sexual assault under the DoD "confidentiality policy" (restricted reporting). In this instance, absolutely no information in identifiable form is collected at all. Requesting information on themselves is a further protection afforded to the individual in this instance as the inability of the

SADMS to be able to provide this would be de facto verification of the legitimacy (and effectiveness) of the DoD confidentiality policy to the requesting individual.

17. **Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.**

N/A with respect to SADMS. This information will have been provided to the victim prior to it being gathered into the source systems.

18. **Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.**

Appropriate administrative, technical and physical safeguards have been established to ensure that records in the SADMS are protected from unauthorized alteration or disclosure and that privacy and confidentiality is preserved and protected. All records are maintained in areas accessible only to authorized personnel who have an official need for access in order to perform their assigned responsibilities and duties. Automated records are further protected by assignment of user identification and passwords managed by the Army via AKO authentication to protect the system from unauthorized access. The system employs a DoD Secure Socket Layer (SSL) certificate for encryption to provide further protection from unauthorized access. Direct system access to personal identifying information (PII) is restricted to only those individuals in or supporting the Headquarters Department of the Army HQDA) Sexual Assault Prevention and Response (SAPR) Program Office will be authorized direct system access to PII contained in the SADMS as needed to discharge their SAPR Program management responsibilities. Personnel with direct system access to personal identifying data within SADMS will receive detailed and continuous training on proper handling and safeguarding of this information. Likewise, no PII contained in SADMS will be disclosed in response to any internal request for information unless specifically approved for release first by the functional system owner(s) of the data and then by either the Assistant Deputy Chief of Staff, G-1 or the Deputy Assistant Secretary of the Army for Human Resources, either of whom must personally determine that the requester's need to know is at least equal to, if not greater than, the potential impact of divulging the PII. Limiting SADMS access and disclosure authority will ensure that information management processes are firmly established across this small population of users.

Unauthorized disclosure of personal identifying information will not be tolerated and personnel responsible for this disclosure may be subject to criminal prosecution under federal law or the Uniform Code of Military Justice.

19. **Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 16, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.**

A System of Records notice (A0600–20 DCS, G–1) was initially published in the Federal Register on 25 October 2005 and resulted in over 5,700 comments being submitted during the 30 day public comment period. A consolidated response to the concerns common among these comments has been developed

and is nearing completion of its staffing. As a result of these comments, the initial systems notice is being amended and is likewise nearing completion of its staffing prior to being re-published in the Federal Register.

20. **Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.**

The Army considered four discreet potential privacy risks in designing and developing the Sexual Assault Data Management System: 1) unauthorized access; 2) inaccurate information; 3) privacy and due process right protection; and 4) unauthorized disclosure.

In response to the risk of unauthorized access to the sensitive information that system records within SADMS will contain (not just the PII, but also the sensitive nature of why it is being collected), the Army is taking a "defense in depth" approach to protecting this information. Physical (e.g., data stored on accredited servers in the Pentagon), technical (e.g., encryption; password protection) and procedural (e.g., physical access to data based on duty position) safeguards are employed in series to ensure only those personnel that demonstrated "need to know" can access information contained within SADMS.

In response to the risk presented by including inaccurate information in the system, the Army plans to correlate information from authoritative sources only and then on an extremely narrow axis – by relying on a combination of personal identifying data elements. Additionally, the SADMS subjects this information to a second layer of data accuracy validation by "checking" the information against personnel authoritative source data in the Integrated Total Army Personnel Database (ITAPDB) and Defense Enrollment Eligibility Reporting System (DEERS). The exceptionally sensitive nature of the information being gathered and connected within SADMS dictates that utmost care be taken to ensure disparate data threads be properly matched 100% of the time.

In response to the risk of violating the rights of the individuals involved in a sexual assault incident; the Army is relying on redundant and parallel protective steps to ensure the individual rights of all parties are vigorously protected. For instance, victim identities are included only when they opt to pursue unrestricted reporting (process a Service member uses to disclose, without requesting confidentiality or restricted reporting, that he or she is the victim of a sexual assault. Under these circumstances, the victim's report and any details provided to healthcare providers, the SARC, a VA, command authorities, or other persons are reportable to law enforcement and may be used to initiate the official investigative process) of the incident. When they choose to report pursuant to the DoD Confidentiality policy (restricted reporting), no personal identifying information is even collected to be passed to SADMS. Alleged offender identities are not included in feeder system data threads to SADMS unless the final report of investigation (Final ROI) determines that charges are founded at the absolute earliest. Procedures are also in place to assure complete record destruction is certified back to the Army CID in instances where courts direct investigative or other records be expunged.

In response to the risk presented by unauthorized disclosure of information contained within SADMS, the Army is taking a multi-pronged approach to mitigating this concern involving: 1) Required and repetitive training/education opportunities; 2) Requirement to execute formal nondisclosure agreements by any and all parties with direct system access to SADMS records containing personal identifying information; and 3) a process requiring targeted senior executive

(SES level) review and explicit approval of requests for PII level detail on sexual assault incidents to both extract and then release the information. This multi-faceted approach to safeguarding personal identifying information provides redundant protections to both the individual identities and institutions involved in the collection and management of this highly personal and sensitive information.

The Army is carefully considering and continually planning and reviewing ways to protect the privacy of individuals involved in sexual assault incidents. More importantly, the activities involved fully understand that this is a dynamic problem and there will likely be an enduring need to analyze the policies and procedures in place to deal with the personal information involved to assure its complete protection.

21. **State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.**

Information contained within the Sexual Data Management System (SADMS) is classified as (Sensitive But Unclassified) and is effectively treated as FOR OFFICIAL USE ONLY (FOUO) IAW guidance set forth in AR 380-5, DA Information Security Program (29 Sep 00). Publication of this PIA in full form is completely warranted and supported.